IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF TEXAS

DALLAS DIVISION

CLINT THOMSON, JUSTIN WILLIAMS, and DEREK SELDERS individually and on behalf of all other similarly situated,	§	Case No. _____
Plaintiffs,	§	Demand for Jury Trial
v.	§	
EQUIFAX INC.,	§	
Defendant.	§	

PLAINTIFFS' COMPLAINT – CLASS ACTION

Plaintiffs Clint Thomson, Justin Williams, and Derek Selders (hereinafter, collectively, "Plaintiffs"), individually and on behalf of the Classes defined below, allege the following against Equifax Inc. ("Equifax") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE CASE

1. Plaintiffs file this complaint on behalf of themselves and on behalf of millions of consumers in the Texas as a class action against Equifax for failing to protect and maintain the confidentiality of those consumers' personal identification and credit information which Equifax collected in connection its business as a consumer credit reporting agency and for failing to provide timely, accurate and adequate notice to those consumers that their information had been stolen and the details of the theft.

2. Plaintiffs seek compensation from Equifax in an amount which will ensure that all consumers who are victims of the theft shall receive the benefit of independent third-party credit repair and monitoring services and other monetary compensation for damages resulting from such theft.

PARTIES

3. Plaintiff Clint Thomson ("Thomson") is a resident of Dallas County, Texas.

4. Plaintiff Justin Williams ("Williams") is a resident of Dallas County, Texas.

5. Plaintiff Derek Selders ("Selders") is a resident of Dallas County, Texas.

6. Defendant Equifax Inc. ("Equifax") is a Georgia corporation with its headquarters located at 1550 Peachtree Street NE Atlanta, Georgia 30309 and with multiple offices located within this District including at 6333 State Highway 161, Irving, Texas 75038 and 14755 Preston Road, Dallas, Texas 75254. Equifax operates through numerous subsidiaries, including Equifax Information Services, LLC, Equifax Consumer Services, LLC, Equifax Services, Inc., all of which acted and act as agents of Equifax or in concert with Equifax as alleged in this Complaint. Equifax may be served through its registered agent Prentice-Hall Corporation System, 211 E. 7th Street, Suite 620, Austin, Texas 78701.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332. As to diversity jurisdiction under 28 U.S.C. § 1332(a), the matter in controversy exceeds the sum or value of $75,000 exclusive of interest and costs and is between citizens of different States. As to jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), the matter in controversy exceeds the sum or value of $5 million, exclusive of interest, and costs, and is a class action in which any member of the class of approximately 143 million plaintiffs is a citizen of a

State different from that of Equifax. The claims asserted involve matters of national or interstate interest, will be governed by federal law and by generalized state laws of negligence, has a distinct nexus with this forum in part due to its extensive business operations and offices in Texas, including in the Dallas-Fort Worth and Houston metropolitan areas.

8. This Court has personal jurisdiction over Equifax, because Equifax maintains offices in Texas, regularly conducts business in Texas, has sufficient minimum contacts in Texas, and has registered to do business in Texas with the Texas Secretary of State. Equifax intentionally availed itself of this jurisdiction by marketing and selling products and services and by accepting and processing payments for those products and services within Texas and by maintaining personal and credit information on millions of consumers who reside in Texas who were affected by the data theft described below.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b), because Equifax is subject to personal jurisdiction in this District, it maintains offices in this District, a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District, and millions of consumers affected by the Data Theft reside in this District.

FACTUAL BACKGROUND

10. Equifax is a consumer credit-reporting company. It collects and aggregates information on hundreds of millions of individual consumers and businesses in the United States and worldwide. Equifax maintains databases containing personal identification information and the financial history of U.S. consumers and businesses.

11. Equifax obtains consumer data about names and aliases, Social Security numbers, driver's license numbers, birthdates, current and former addresses, credit dispute information, credit card numbers and usage, loans and loan payments child support, credit limits, rent,

utilities, and employer history. Equifax obtains its data from credit card companies, banks, retailers, and lenders who report on the credit activity of individuals to credit reporting agencies and by purchasing public records.

12. On September 7, 2017, Equifax issued a press release, publicly revealing for the first time that criminal third parties had gained access to consumer data maintained by Equifax. The press release stated:

> Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.
>
> The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents. Equifax will work with UK and Canadian regulators to determine appropriate next steps. The company has found no evidence that personal information of consumers in any other country has been impacted.
>
> Equifax discovered the unauthorized access on July 29 of this year and acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.
>
> "This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes," said Chairman and Chief Executive Officer, Richard F. Smith. "We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations. We also are focused on consumer protection and have

developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident."

Equifax has established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection. The offering, called TrustedID Premier, includes 3-Bureau credit monitoring of Equifax, Experian and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers - all complimentary to U.S. consumers for one year. The website also provides additional information on steps consumers can take to protect their personal information. Equifax recommends that consumers with additional questions visit www.equifaxsecurity2017.com or contact a dedicated call center at 866-447-7559, which the company set up to assist consumers. The call center is open every day (including weekends) from 7:00 a.m. – 1:00 a.m. Eastern Time.

In addition to the website, Equifax will send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted. Equifax also is in the process of contacting U.S. state and federal regulators and has sent written notifications to all U.S. state attorneys general, which includes Equifax contact information for regulator inquiries.

Equifax has engaged a leading, independent cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again.

CEO Smith said, "I've told our entire team that our goal can't be simply to fix the problem and move on. Confronting cybersecurity risks is a daily fight. While we've made significant investments in data security, we recognize we must do more. And we will."

13. Equifax admits in the press release the following:

a. Equifax discovered the security breach on July 29, 2017.

b. The hackers gained access by exploiting an Equifax-maintained U.S. website application vulnerability from May to July 2017.

c. The hackers were then able to gain access to files which included information on U.S. consumers, including names, Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers, and certain dispute documents with personal identifying information.

d. The breach potentially affects 143 million U.S. consumers.

14. It is estimated that approximately 12 million Texas consumers will be affected by the breach.

15. Personal identification and credit information is often misused by cybercriminals to engage in identity theft and financial fraud. Cybercriminals also sell such information on the Dark Web to other criminals who then use the information to engage in identify theft and financial fraud.

16. The stolen information can be used by to obtain fake identification cards and driver's licenses, to open fraudulent financial accounts such as credit cards or loans, to obtain medical care under false pretenses, to poach health insurance coverage, to file for fraudulent tax refunds, to file for fraudulent unemployment or Social Security benefits, and to gain access to online accounts.

17. Equifax has identified each of the Plaintiffs as victims who were affected by the data breach.

18. Each of the Plaintiffs has spent considerable time and effort monitoring their financial accounts after the data breach was publicly disclosed by Equifax.

19. Plaintiffs and the Class members have suffered actual injury in the form of damages to and diminution in the value of their personal and credit information and imminent and impending injury arising from the substantially increased risk of future financial fraud, identity theft, and other misuse by hackers and identity thieves.

20. Plaintiffs and the Class members have a continuing interest in ensuring that their private personal and credit information, which remains in the possession of Equifax, is protected and safeguarded from future breaches.

21. Equifax was well-aware, or reasonably should have been aware, that the personal and financial information collected, maintained, and stored in by it is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

22. Major data breaches where hackers have gained access to private consumer information have been extensively reported on by the media and studied by those in the cybersecurity industry.

23. For example, one of the largest data breaches in history involved a major Equifax competitor named Experian in 2012 and an Experian subsidiary named Court Ventures. The Experian breach potentially exposed to hackers up to 200 million records containing personal and financial information, including Social Security numbers, of American consumers.

24. As another example, in 2008 and 2009, Heartland Payment Systems suffered a data breach which compromised about 130 million records, which included consumer credit card data.

25. As further examples, TK/TJ Maxx had 94 million records compromised by hackers in 2007; the Sony PlayStation Network had 77 million records compromised in 2010; Sony Online Entertainment had 24.6 million records compromised in 2011; Evernote had 50 million records compromised in 2013; Living Social had 50 million records compromised in 2013; Target had 70 million records compromised in 2013; eBay had 145 million records compromised in 2014; Home Depot had 56 million records compromised in 2014; JPMorgan Chase had 76 million records compromised in 2014; and Anthem had 80 million records compromised in 2015.

26. Despite its knowledge of the risks to its systems and susceptibility to cyberattacks, Equifax maintained insufficient and inadequate systems to protect the information of Plaintiffs and the Class members.

27. Equifax knew, or reasonably should have known, of the importance of safeguarding the private information maintained in its databases and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on individual consumers because of a breach.

28. Equifax knew, or reasonably should have known, of the significant number of consumers on whom information was collected, and thus, the significant number of consumers who would be harmed by a breach of Equifax's systems.

29. Despite all the publicly available information of the repeated breaches of private consumer information incurred through the financial databases of third parties, Equifax's approach to maintaining the privacy and security of the information of Plaintiffs and Class members was at a minimum negligent or grossly negligent.

30. The consequences of Equifax's failure to keep Plaintiffs' and Class members' information secure are severe.

31. Consumer victims of the breach will never be 100% certain while they are alive that they will not be a victim of identity theft or financial fraud so long as their private identification and financial information is easily accessible to criminals. And even after death, identification and financial information can be used by criminals to impersonate the deceased.

32. Plaintiffs and Class members now a lifetime of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and the Class members

are incurring and will continue to incur such damages in addition to any fraudulent use of their personal information.

33. The personal information of Plaintiffs and Class members is private and sensitive in nature and was inadequately protected by Equifax. Equifax did not obtain Plaintiffs' and Class members' consent to disclose their personal information to any other person as required by applicable law and industry standards.

34. The Equifax data breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiffs' and Class members' personal information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' personal information to protect against reasonably foreseeable threats to the security or integrity of such information.

35. Equifax had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

36. Had Equifax remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the industry, Equifax would have prevented the data breach and, ultimately, the theft of the personal consumer information.

37. As a direct and proximate result of Equifax's wrongful actions and inaction and the resulting data breach, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as

work and effort to mitigate the actual and potential impact of the data breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, subscribing to and paying for third party independent credit monitoring services, and filing police reports. This time has been, and will be, lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a credit reporting agency's malfeasance.

38. Equifax's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class members' personal information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. increased likelihood of unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal information's being placed in the hands of criminals or misused via the sale of Plaintiffs' and Class members' information on the black market and Dark Web;

d. the untimely and inadequate notification of the data breach;

e. the improper disclosure of their personal information;

f. loss of privacy;

g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

h. ascertainable losses in the form of deprivation of the value of their personal information, for which there is a well-established national and international market;

i. ascertainable losses in the form of the loss of cash back or other benefits because of their potential inability to use certain accounts and cards affected by the data breach;

j. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations;

k. ascertainable losses in the form of paid subscription fees to third party independent credit monitoring and identity theft protection services; and,

l. the loss of productivity and value of their time spent to address attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling, and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with all such issues resulting from the data breach.

39. Equifax has not offered customers any meaningful independent third-party credit monitoring and identity theft protection services, even though it is well known and acknowledged by the government that damage and fraud from a data breach can take years to occur. As a result, Plaintiffs and Class members are left to their own actions to protect themselves from the financial damage Equifax has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Equifax's actions have created for Plaintiffs and Class members, is ascertainable and is a determination appropriate for the trier of fact. Equifax has also not offered to cover any of the damages sustained by Plaintiffs or Class members.

40. While the personal information of Plaintiffs and Class has been stolen, Equifax continues to hold personal information of consumers, including that of Plaintiffs and Class

members. Particularly because Equifax and has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and Class members have an undeniable interest in insuring that their personal information is secure, remains secure, is properly and promptly destroyed and is not subject to further theft and that an independent third-party credit monitoring and identify theft service is utilized to ensure that personal consumer information is not misused.

CLASS ACTION ALLEGATIONS

41. Plaintiffs' seeks relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to FED. R. CIV. P. 23, Plaintiffs seeks certification of a class of Texas consumers defined as follows:

> All persons residing in the State of Texas whose personal or financial information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017 (the "Texas Class").

42. Excluded from the Class are Equifax and any of its affiliates, parents, or subsidiaries; all employees of Equifax; all persons who make a timely election to be excluded from the Class; government entities; the judges to whom this case is assigned and their immediate family and court staff, and all jurors and alternate jurors who sit on the case.

43. The precise number of aggrieved consumers in Texas can be determined based on Equifax's consumer database and is currently estimated at 12 million Texas consumers.

44. Plaintiffs hereby reserve the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

45. Each of the proposed Classes meets the criteria for certification under Federal Rule of Civil Procedure 23.

46. Numerosity**. FED. R. CIV. P. 23(a)(1).** Consistent with FED. R. CIV. P. 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, it has been estimated that there are at least 12 million Texas consumers whose personal information was compromised by the Equifax data breach. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, or published notice.

47. Commonality**. FED. R. CIV. P. 23(a)(2) and (b)(3).** Consistent with FED. R. CIV. P. 23(a)(2)'s and 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether Equifax had a duty to protect consumer personal information;

b. Whether Equifax knew or should have known of the susceptibility of their data security systems to a data breach;

c. Whether Equifax's security measures to protect their systems were reasonable considering the measures recommended by data security experts;

d. Whether Equifax was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Equifax's failure to implement adequate data security measures allowed the breach to occur;

f. Whether Equifax's conduct constituted deceptive trade practices under Texas law;

g. Whether Equifax's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the personal information of Plaintiffs and Class members;

h. Whether Plaintiffs and Class members were injured and suffered damages or other acceptable losses because of Equifax's failure to reasonably protect its systems and data network; and

i. Whether Plaintiffs and Class members are entitled to relief.

48. Typicality**. FED. R. CIV. P. 23(a)(3).** Consistent with FED. R. CIV. P. 23(a)(3), Plaintiffs' claims are typical of those of other Class members. Plaintiffs had their personal information compromised in the Equifax data breach. Plaintiffs' damages and injuries are akin to other Class members and Plaintiffs seeks relief consistent with the relief of the Class.

49. **Adequacy. FED. R. CIV. P. 23(a)(4).** Consistent with FED. R. CIV. P. 23(a)(4), Plaintiffs are adequate representatives of the Class, because Plaintiffs are members of the Class and are committed to pursuing this matter against Equifax to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

50. Superiority**. FED. R. CIV. P. 23(b)(3).** Consistent with FED. R. CIV. P 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual Plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Equifax, and thus, individual litigation to redress Equifax's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action

device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

51. Injunctive **and Declaratory Relief.** Class certification is also appropriate under FED. R. CIV. P. 23(b)(2) and (c). Defendant, through its uniform conduct, has acted or refused to act on grounds generally applicable to the Class members, making injunctive and declaratory relief appropriate to the Class members as a whole.

52. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification, because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Equifax failed to timely notify the public of the data breach;

b. Whether Equifax owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their personal information;

c. Whether Equifax's security measures were reasonable considering data security recommendations, and other measures recommended by data security experts;

d. Whether Equifax failed to adequately comply with industry standards amounting to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard the personal information of Plaintiffs and the Class members; and,

f. Whether adherence to data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

53. Finally, all members of the proposed Classes are readily ascertainable. Equifax has access to information regarding he data breach, the time period of the data breach, and which individuals were potentially affected. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

CAUSES OF ACTION

FIRST CLAIM FOR RELIEF

NEGLIGENCE
ON BEHALF OF PLAINTIFFS AND THE CLASS MEMBERS

54. Plaintiffs restate and reallege all prior factual allegations as if fully set forth herein.

55. Upon accepting and storing the personal information of Plaintiffs and the Class Members in its computer systems and on its networks, Equifax undertook and owed a duty to Plaintiffs and the Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Equifax knew that the personal information was private and confidential and should be protected as private and confidential.

56. Equifax owed a duty of care not to subject Plaintiffs and the Class members, and their personal information, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

57. Equifax owed numerous duties to Plaintiffs and to the Class members, including the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the personal information of Plaintiffs and the Class members in its possession;

b. to protect the personal information of Plaintiffs and the Class members using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

58. Equifax also breached its duty to Plaintiffs and the Class Members to adequately protect and safeguard their personal information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured personal information. Furthering their dilatory practices, Equifax failed to provide adequate supervision and oversight of the personal information of Plaintiffs and the Class members with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather personal information of Plaintiffs and the Class members, misuse the personal information of Plaintiffs and the Class members, and intentionally disclose it to others without consent.

59. Equifax knew, or should have known, of the risks inherent in collecting and storing personal information of Plaintiffs and the Class members, the vulnerabilities of its data security systems, and the importance of adequate security. Equifax knew about numerous, well-publicized data breaches, including the breach at Experian.

60. Equifax knew, or should have known, that their data systems and networks did not adequately safeguard personal information of Plaintiffs and the Class members.

61. Equifax breached its duties to Plaintiffs and the Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the personal information of Plaintiffs and the Class members.

62. Because Equifax knew that a breach of its systems would damage millions of individuals, including Plaintiffs and the Class members, Equifax had a duty to adequately protect their data systems and the personal information of Plaintiffs and the Class members contained thereon.

63. Equifax had a special relationship with Plaintiffs and the Class members. Plaintiffs' and the Class members' willingness to entrust Equifax with their personal information was predicated on the understanding that Equifax would take adequate security precautions. Moreover, only Equifax had the ability to protect its systems and the personal information of Plaintiffs and the Class members it stored on them from attack.

64. Equifax's own conduct also created a foreseeable risk of harm to Plaintiffs and the Class members and personal information of Plaintiffs and the Class members. Equifax's misconduct included: (1) failing to secure its systems, despite knowing their vulnerabilities, (2) failing to comply with industry standard security practices, (3) failing to implement adequate system and event monitoring, and (4) failing to implement the systems, policies, and procedures necessary to prevent this type of data breach.

65. Equifax also had independent duties under state and federal laws that required Equifax to reasonably safeguard the personal information of Plaintiffs and the Class members and promptly notify them about any data breach.

66. Equifax breached its duties to Plaintiffs and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the personal information of Plaintiffs and the Class members;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols, and practices sufficient to protect the personal information of Plaintiffs and the Class members both before and after learning of the data breach;

d. by failing to comply with the minimum industry data security standards during the period of the data breach; and

e. by failing to timely and accurately disclose that the personal information of Plaintiffs and the Class members had been improperly acquired or accessed as required by the Texas Identity Theft Enforcement and Protection Act (TEX. BUS. & COMM. CODE Ch. 521) and other applicable law.

67. Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect the personal information of Plaintiffs and the Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure the personal information of Plaintiffs and the Class members during the time it was within Equifax possession or control.

68. The law further imposes an affirmative duty on Equifax to timely disclose the unauthorized access and theft of personal information of Plaintiffs and the Class members to Plaintiffs and the Class members so that Plaintiffs and the Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their personal information.

69. Equifax breached its duty to notify Plaintiffs and the Class Members of the unauthorized access by waiting several months after learning of the breach to issue a public press release which for the first time notified the public of the data breach and then by failing to provide any detailed information regarding the breach.

70. Instead, its executives disposed of at least $1.8 million worth of shares in the company after Equifax learned of the data breach but before it was publicly announced.

71. To date, Equifax has not provided sufficient information to Plaintiffs and the Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class members.

72. Through Equifax's acts and omissions, including Equifax's failure to provide adequate security and its failure to protect the personal information of Plaintiffs and the Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure the personal information of Plaintiffs and the Class members during the time it was within Equifax's possession or control.

73. Further, through its failure to provide timely and clear notification of the data breach to consumers, Equifax prevented Plaintiffs and the Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

74. Upon information and belief, Equifax improperly and inadequately safeguarded the personal information of Plaintiffs and the Class members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Equifax's failure to take proper security measures to protect sensitive personal information of Plaintiffs and the Class members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of the personal information of Plaintiffs and the Class members and the likely dissemination of the personal information of Plaintiffs and the Class members on the Dark Web and the black market.

75. Equifax's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the personal information of Plaintiffs and the Class members; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to the personal information of Plaintiffs and the Class members; and failing to provide Plaintiffs and the Class

members with timely and sufficient notice that their sensitive personal information had been compromised.

76. Neither Plaintiffs nor the Class members contributed to the data breach and subsequent misuse of their personal information.

77. As a direct and proximate cause of Equifax's conduct, Plaintiffs and the Class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the personal information of Plaintiffs and the Class members; damages arising from Plaintiffs' and the Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the data breach and/or false or fraudulent charges stemming from the data breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, paying for independent third party subscription services for credit monitoring and identity theft prevention, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

SECOND CLAIM FOR RELIEF

NEGLIGENCE PER SE
ON BEHALF OF PLAINTIFFS AND THE CLASS MEMBERS

78. Plaintiffs restate and reallege all prior factual allegations as if fully set forth herein.

79. The Federal Trade Commission Act of 1914 ("FTC Act") prohibits "unfair or deceptive practices in or affecting commerce," (15 U.S.C. § 45) including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect the personal information of Plaintiffs and the Class members. The FTC publications and orders described above also form part of the basis of Equifax's duty in this regard.

80. Equifax violated the FTC Act by failing to use reasonable measures to protect the personal information of Plaintiffs and the Class members and not complying with applicable industry standards. Equifax's conduct was particularly unreasonable given the nature and amount of personal information it obtained and stored and the foreseeable consequences of a potential data breach at Equifax, including, specifically, the immense damages that would result to Plaintiffs and the Class members.

81. Equifax's violation of the FTC Act constitutes negligence *per se*.

82. Plaintiffs and the Class members are within the class of persons that the FTC Act was intended to protect.

83. The harm that occurred because of the Equifax data breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, because of their failure to employ reasonable data security measures and

avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class members.

84. As a direct and proximate result of Equifax's negligence *per se*, Plaintiffs and the Class members have suffered, and continue to suffer, injuries damages arising from Plaintiffs' and the Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the data breach and/or false or fraudulent charges stemming from the data breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, paying for independent third party subscription services for credit monitoring and identity theft prevention, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

THIRD CLAIM FOR RELIEF

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT ON BEHALF OF PLAINTIFFS AND THE CLASS MEMBERS

85. Plaintiffs restate and reallege all prior factual allegations as if fully set forth herein.

86. As individuals, Plaintiffs and Class member are consumers entitled to the protections of the Fair Credit Reporting Act ("FCRA"). 15 U.S.C. § 1681a(c).

87. Under the FCRA, a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole

or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . .." 15 U.S.C. § 1681a(f).

88. Equifax is a consumer reporting agency under the FCRA because, for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

89. As a consumer reporting agency, the FCRA requires Equifax to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

90. Under the FCRA, a "consumer report" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1). The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Plaintiff's and the Class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing Plaintiff's and the Class members' eligibility for credit.

91. As a consumer reporting agency, Equifax may furnish a consumer report only under the limited circumstances set forth in 15 U.S.C. § 1681b "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities or computer hackers such as those who accessed the personal information of Plaintiffs and the Class members. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers.

92. Equifax furnished Plaintiffs' and the Class members' consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

93. The FTC has pursued enforcement actions against consumer reporting agencies under the FCRA for failing to "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the" FCRA, relating to data breaches.

94. Equifax willfully and/or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. The willful and reckless nature of Equifax's violations is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further,

Equifax touts itself as an industry leader in breach prevention; thus, Equifax was aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

95. Equifax also acted willfully and recklessly because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary on the Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix to Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiffs and the Class members of their rights under the FCRA.

96. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and the Class members' personal information for no permissible purposes under the FCRA.

97. Plaintiffs and the Class members have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiffs and each of the Class members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

98. Plaintiffs and the Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2) & (3).

FOURTH CLAIM FOR RELIEF

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT ON BEHALF OF PLAINTIFFS AND THE CLASS MEMBERS

99. Plaintiffs restate and reallege all prior factual allegations as if fully set forth herein.

100. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

101. Equifax's negligent conduct provided a means for hackers to obtain access to the Plaintiffs' and Class members' personal information and consumer reports for no permissible purposes under the FCRA.

102. Plaintiffs and the Class members have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiffs and each of the Class members are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

103. Plaintiffs and the Nationwide Class member are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

FIFTH CLAIM FOR RELIEF

DECLARATORY JUDGMENT
ON BEHALF OF PLAINTIFFS AND THE CLASS MEMBERS

104. Plaintiffs restate and reallege all prior factual allegations as if fully set forth herein.

105. Plaintiffs and the Class members entered into an implied contract with Equifax that required Equifax to provide adequate security for the personal information of Plaintiffs and the Class members which it collected and maintained. Alternatively, Plaintiffs and Class members were intended third party beneficiaries to contracts between providers of their personal information and Equifax. Equifax owes duties of care to Plaintiffs and Class members that require it to adequately secure the personal information of Plaintiffs and the Class members.

106. Equifax still possesses the personal information of Plaintiffs and the Class members.

107. Equifax has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems.

108. Accordingly, Equifax has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class members. In fact, now that Equifax's lax approach towards data security has become public, the personal information in its possession has become more vulnerable.

109. Actual harm has arisen in the wake of the Equifax Data Breach regarding Equifax's contractual obligations and duties of care to provide data security measures to Plaintiffs and the Class members.

110. Plaintiffs and the Class members, therefore, seek a declaration that (a) Equifax's existing data security measures do not comply with its contractual obligations and duties of care

and (b) in order to comply with its contractual obligations and duties of care, Equifax must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting consumer personal information by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. purging, deleting, and destroying in a reasonable secure manner PII not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating consumers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps consumers must take to protect themselves.

SIXTH CLAIM FOR RELIEF

VIOLATION OF THE TEXAS DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT
ON BEHALF OF PLAINTIFFS AND THE CLASS MEMBERS

111. Plaintiffs restate and reallege all prior factual allegations as if fully set forth herein.

112. Equifax is engaged in, and their acts and omissions affect, trade and commerce pursuant to the Texas Deceptive Trade Practices—Consumer Protection Act ("DTPA"). TEX. BUS. & COMM. CODE Ch. 17.

113. Plaintiffs and the Class members are "consumers" as defined by the DTPA. TEX. BUS. & COMM. CODE § 17.45(4).

114. Plaintiffs and the Class members entrusted Equifax with their personal information.

115. Equifax engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the DTPA, TEX. BUS. & COMM. CODE § 17.46:

a. failure to maintain adequate computer systems and data security practices to safeguard the personal information of Plaintiffs and the Class members;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft;

c. failure to timely and accurately disclose the data breach to Plaintiffs and the Class members;

d. continued acceptance of the personal information of Plaintiffs and the Class members and storage of other personal information after Equifax knew or should have known of the security vulnerabilities of the systems that were exploited in the data breach;

e. continued acceptance of the personal information of Plaintiffs and the Class members and storage of other personal information after Equifax knew or should have known of the Data Breach and before it allegedly remediated the Breach; and

f. violating the FTCA.

116. Equifax violated at least the following provisions of the DTPA: TEX. BUS. & COMM. CODE § 17.46(a) and (b)(5, 7, 12, 22, and 24).

117. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the personal information of Plaintiffs and the Class members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

118. As a direct and proximate result of Equifax's violation of the DTPA, Plaintiffs and the Class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the personal information of Plaintiffs and the Class members; damages arising from Plaintiffs' and the Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the data breach and/or false or fraudulent charges stemming from the data breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, paying for independent third party subscription services for credit monitoring and identity theft prevention, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

119. Also as a direct result of Equifax's knowing violation of the DTPA, Plaintiffs and Class members are entitled to treble damages as well as injunctive relief, including, but not limited to:

a. Ordering that Equifax engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Equifax engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Equifax segment consumer personal information by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. Ordering that Equifax purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Equifax conduct regular database scanning and securing checks;

g. Ordering that Equifax routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Equifax to meaningfully educate consumers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps consumers must take to protect themselves.

120. Plaintiffs bring this action on behalf of themselves and for the Class Members for the relief requested above and for the public benefit in order to promote the public interest in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs and the Class members and the public from Equifax's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable, and unlawful practices. Equifax's

wrongful conduct has had widespread impact on the public at large and on consumers within the State of Texas.

121. Plaintiffs and Class members are entitled to a judgment against Equifax for actual and consequential damages, treble damages, and attorneys' fees pursuant to the DTPA, costs, and such other further relief as the Court deems just and proper.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Equifax as follows:

a. For an Order certifying the Classes, as defined herein, and appointing Plaintiffs and their Counsel to represent the Class members;

b. For equitable relief enjoining Equifax from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the personal information of Plaintiffs and the Class members and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and Class members;

c. For equitable relief compelling Equifax to use appropriate cybersecurity methods and policies with respect to consumer data collection, storage, and protection and to disclose with specificity to Class members exactly which personal information was compromised;

d. For an award of damages, as allowed by law in an amount to be determined by a jury;

e. For an award of attorneys' fees, costs, and litigation expenses, as allowable by law;

f. For pre- and post-judgment interest on all amounts awarded; and

g. Such other and further relief as this court may deem just and proper.

JURY DEMAND

Plaintiffs demand a jury trial on all issues so triable.

Dated: September 14, 2017

Respectfully submitted,

BUETHER JOE & CARPENTER, LLC

By: */s/ Christopher M. Joe*
Christopher M. Joe
State Bar No. 00787770
Chris.Joe@BJCIPLaw.com
Eric W. Buether
State Bar No. 03316880
Eric.Buether@BJCIPLaw.com
Brian A. Carpenter
State Bar No. 03840600
Brian.Carpenter@BJCIPLaw.com

1700 Pacific Avenue
Suite 4750
Dallas, Texas 75201
Telephone: (214) 466-1272
Facsimile: (214) 635-1828

ATTORNEYS FOR PLAINTIFFS CLINT THOMSON, JUSTIN WILLIAMS AND DEREK SELDERS INDIVIDUALLY AND ON BEHALF OF ALL OTHER SIMILARLY SITUATED CLASS MEMBERS